

Appl. No. : 09/787,784

Examiner : Unknown

IN THE CLAIMS:

Please delete Claims 1-8 without prejudice.

Please add the following new claims:

9. A data transfer system comprising:

a key facility;

a sender facility configured to communicate with the key facility, the sender facility including:

a first encryption module to encrypt data for an intended recipient, a partitioning module to split the data into encrypted parts such that no part is decryptable on its own,

a second encryption module to encrypt at least one of the parts for a third party to produce a further encrypted part,

a combiner to combine the further encrypted part and a remaining encrypted part to produce a data block, and

a first transmitter to send the data block; and

a receiver facility configured to communicate with the key facility, the receiver facility including:

a receiver to receive the data block, and a command module to request decryption of the further encrypted part by the key facility;

wherein the key facility further comprises a first decryption module to decrypt the further encrypted part and a second transmitter to send it to the receiver facility; and

wherein the receiver facility further comprises a second decryption module to decrypt the encrypted part and the decrypted further encrypted part provided by the key facility.

10. The system of Claim 9, wherein the send facility includes a signature module to sign the data block.

11. The system of Claim 9, wherein the first transmitter is configured to send the data block to the key facility, and wherein the key facility further includes a receiver to receive the data block and to forward the data block to the receiver facility.

Appl. No. : **09/787,784**
Examiner : **Unknown**

12. The system of Claim 11, wherein the key facility further includes a log module to log receipt of the data block.

13. The system of Claim 9, wherein the receiver facility is configured to communicate with the key facility and the sender facility, and wherein the first transmitter is configured to send the data block to the receiver facility, the receiver facility further including a receiver to receive the data block.

14. The system of Claim 13, wherein the key facility further includes a log module to log receipt of the further encrypted part.

15. The system of Claim 9, wherein the key facility further includes a log module to log receipt of the request for decryption of the further encrypted part as proof of delivery of the data block to the receiver facility.

16. The system of Claim 15, wherein the sender facility further includes a delivery module to request proof of delivery information from the key facility.

17. The system of Claim 9, wherein the third party is the key facility.

18. A method of data transfer, comprising:

at a sender facility:

encrypting data for an intended recipient,

splitting the data into encrypted parts such that no part is decryptable on its own,

encrypting at least one of the parts for a third party to produce a further encrypted part,

combining the further encrypted part and a remaining encrypted part to produce a data block, and

sending the data block;

Appl. No. : 09/787,784
Examiner : Unknown

at a receiver facility:

receiving the data block, and

requesting decryption of the further encrypted part by a key facility;

at the key facility:

decrypting the further encrypted part, and

transmitting the decrypted further encrypted part to the receiver facility;

and

at the receiver facility:

decrypting the encrypted part and the decrypted further encrypted part
provided by the key facility.

19. The method of Claim 18, further comprising signing the data block at the sender facility.

20. The method of Claim 18, wherein the sending at the sender facility is configured to send the data block to the key facility, and wherein the method further comprises at the key facility receiving the data block and forwarding the data block to the receiver facility.

21. The method of Claim 20, further comprising, at the key facility, logging receipt of the data block.

22. The method of Claim 18, wherein the sending at the sender facility is configured to send the data block to the receiver facility, and wherein the method further comprises, at the receiver facility, receiving the data block.

23. The method of Claim 22, further comprising, at the key facility, logging receipt of the further encrypted part.

24. The method of Claim 18, further comprising, at the key facility, logging receipt of the request for decryption of the further encrypted part as proof of delivery of the data block to the receiver facility.

25. The method of Claim 24, further comprising, at the sender facility, requesting proof of delivery information from the key facility.

26. The method of Claim 18, wherein the third party is the key facility.

27. A data transfer system comprising:

a key facility;

a sender facility configured to communicate with the key facility, the sender facility including a first encryption module to encrypt data for an intended recipient, a partitioning module to split the data into encrypted parts such that no part is decryptable on its own, a second encryption module to encrypt at least one of the parts for the key facility to produce a further encrypted part, a combiner to combine the further encrypted part and a remaining encrypted part to produce a data block, a signature module to sign the data block and a first transmitter to send the data block to the key facility; and

a receiver facility configured to communicate with the key facility, the receiver facility including a receiver to receive the data block from the key facility, and a command module to request decryption of the further encrypted part by the key facility;

wherein the key facility further comprises a receiver to receive the data block from the sender facility and to forward the data block to the receiver facility, a first log module to log recipient of the data block from the sender facility, a second log module to log receipt of the decryption request from the receiver facility as proof of delivery of the data block to the receiver facility, a first decryption module to decrypt the further encrypted part on receipt of the request from the receiver facility and a second transmitter to send the decrypted further encrypted part to the receiver facility;

wherein the receiver facility further comprises a second decryption module to decrypt the encrypted part and the decrypted further encrypted part provided by the key facility; and

wherein the sender facility further includes a delivery module to request proof of delivery information from the key facility.

Appl. No. : 09/787,784
Examiner : Unknown

28. A data transfer system comprising:

a key facility;

a sender facility configured to communicate with the key facility and a receiver facility, the sender facility including a first encryption module to encrypt data for an intended recipient, a partitioning module to split the data into encrypted parts such that no part is decryptable on its own, a second encryption module to encrypt at least one of the parts for the key facility to produce a further encrypted part, a combiner to combine the further encrypted part and a remaining encrypted part to produce a data block, a signature module to sign the data block and a first transmitter to send the data block to the receiver facility;

wherein the receiver facility is configured to communicate with the key facility and the sender facility, and the receiver facility includes a receiver to receive the data block from the sender facility, and a command module to request decryption of the further encrypted part by the key facility;

wherein the key facility further comprises a log module to log receipt of the further encrypted part, a first decryption module to decrypt the further encrypted part on receipt of the request from the receiver facility and a second transmitter to send the decrypted further encrypted part to the receiver facility; and

wherein the receiver facility further comprises a second decryption module to decrypt the encrypted part and the decrypted further encrypted part provided by the key facility.

29. A method of transferring data, comprising:

at a sender facility:

encrypting data for an intended recipient, splitting the data into encrypted parts such that no part is decryptable on its own, encrypting at least one of the parts for a key facility to produce a further encrypted part, combining the further encrypted part and a remaining encrypted part to produce a data block, signing the data block and sending the data block to the key facility;

at the key facility:

Appl. No. : 09/787,784
Examiner : Unknown

receiving the data block from the sender facility, forwarding the data block to the receiver facility, and logging receipt of the data block from the sender facility;

at a receiver facility:

receiving the data block from the key facility, and requesting decryption of the further encrypted part by the key facility;

at the key facility:

logging receipt of the decryption request from the receiver facility as proof of delivery of the data block to the receiver facility, decrypting the further encrypted part on receipt of the request from the receiver facility, and sending the decrypted further encrypted part to the receiver facility;

at the receiver facility:

decrypting the encrypted part and the decrypted further encrypted part provided by the key facility; and

at the sender facility:

requesting proof of delivery information from the key facility.

30. A method of transferring data, comprising:

at a sender facility:

encrypting data for an intended recipient, splitting the data into encrypted parts such that no part is decryptable on its own, encrypting at least one of the parts for a key facility to produce a further encrypted part, combining the further encrypted part and a remaining encrypted part to produce a data block, signing the data block and sending the data block to a receiver facility;

at the receiver facility:

receiving the data block from the sender facility, and requesting decryption of the further encrypted part by the key facility;

at the key facility: